JOURNAL OF NUMBER THEORY 34, 198–209 (1990)

Proof of a Conjecture by Erdős and Graham Concerning the Problem of Frobenius

JACQUES DIXMIER

Institut des Hautes Études Scientifiques, 35 route de Chartres, 91440 Bures-sur-Yvette, France

Communicated by R. L. Graham

Received September 16, 1988; revised April 10, 1989

Let $x_1 < x_2 < \cdots < x_b$ be integers $\geqslant 1$ such that $\gcd(x_1, ..., x_b) = 1$. Let S be the additive subsemigroup of $\mathbb{N}$ generated by $x_1, ..., x_b$. Let $G(x_1, ..., x_b)$ be the greatest element of the (finite) set $\mathbb{N} \setminus S$. Let $g(b, a) = \sup G(x_1, ..., x_b)$, where the upper bound is taken over all systems $x_1, ..., x_b$ such that $1 \leqslant x_1 < \cdots < x_b \leqslant a$, $\gcd(x_1, ..., x_b) = 1$. According to a conjecture of Erdös and Graham, it is proved that $g(b, a)$ is roughly equal to $a^2/(b-1)$, and the exact value of $g(b, a)$ is computed when $b-1$ divides a or $a-1$ or $a-2$. It is proved that $S \cap](k-1)a, ka]$ contains at least $\inf(a, kb-k+1)$ elements for $k = 1, 2, ...$.

1. INTRODUCTION

Let $x_1 < x_2 < \cdots < x_b$ be integers $\geqslant 1$ such that $\gcd(x_1, ..., x_b) = 1$. Let S be the additive subsemigroup of $\mathbb{N}$ generated by $x_1, ..., x_b$ (i.e., the set of all sums $y_1 + y_2 + \cdots + y_n$, where every y_i is equal to some x_j). It is well known that S contains all integers from some point onwards. Let n be the smallest integer such that $[n+1, \infty[\subset S$ (all intervals are intervals of integers); let us set, as usual, $n = G(x_1, x_2, ..., x_b)$. The computation of $G(x_1, x_2, ..., x_b)$ ("problem of Frobenius") has given rise to many papers. Let us set, as in [2],

$$g(b, a) = \max G(x_1, x_2, ..., x_b),$$

where the upper bound is taken over all systems of integers $x_1, ..., x_b$ such that $1 \leqslant x_1 < x_2 < \cdots < x_b \leqslant a$ and $\gcd(x_1, ..., x_b) = 1$. It is proved in [2, p. 402], that, for $b \geqslant 2$,

$$\frac{a^2}{b-1} - 5b \leqslant g(b, a) < 2\frac{a^2}{b},$$

and it is conjectured in [3, p. 86] that $g(b, a)$ is roughly equal to $a^2/(b-1)$. We will prove

0022-314X/90 $3.00

THEOREM 1. *One has, for* $2 \leqslant b < a$,

$$\left\lfloor \frac{a-2}{b-1} \right\rfloor (a-b+1) - 1 \leqslant g(b,a) \leqslant \left(\left\lceil \frac{a-1}{b-1} \right\rceil - 1 \right) a - 1.$$

(*For any real number* x, $\lfloor x \rfloor = \sup_{y \in \mathbb{Z},\, y \leqslant x} y$ *and* $\lceil x \rceil = \inf_{y \in \mathbb{Z},\, y \geqslant x} y$).

We will also prove some refinements of Theorem 1 (Theorems 3, 4, 5). Theorems 4, 5 give the exact value of $g(b, a)$ when $b-1$ divides a or $a-1$ or $a-2$.

Numerical experiments suggest the vague idea that not only does S contain all integers from some point onwards, but S becomes denser and denser when one climbs the scale of integers. We will prove

THEOREM 2. *Let* a, b *be integers* $\geqslant 1$, E *a set of* b *integers belonging to* $[1, a]$, *such that* $\gcd E = 1$. *Let* S *be the additive subsemigroup of* $\mathbb{N}$ *generated by* E. *For* $k = 1, 2, \ldots$, *let* $S_k = S \cap [(k-1)a + 1, ka]$. *Then* $\operatorname{Card} S_k \geqslant \inf(a, kb - k + 1)$.

Theorems 1, 3, 4, 5 will be easy consequences of Theorem 2. Also, we will use Theorem 2 in another paper studying partitions.

2. SOME LEMMAS

2.1. LEMMA. *Let* A *be a finite commutative group, additively noted,* B *a subset of* A, *and* b_0 *an element of* B, *with the following property*:

if $b, b' \in B$, *then* $b + b' \in B$, *except possibly if* $b = b' = b_0$.

Then $B = \{b_0\}$, *or* $B = \{0, b_0\}$, *or* B *is a subgroup of* A.

Let B_0 be the subgroup of A generated by b_0, and $B_0' = B \cap B_0$. If $x \in B \setminus B_0'$, one has $x \notin B_0$, whence $x + b_0 \in B \setminus B_0'$; so $x + nb_0 \in B \setminus B_0'$ for every $n \in \mathbb{N}$. So $B \setminus B_0'$ is a union of classes modulo B_0.

Let $\pi: A \to A/B_0$ the canonical map. Let

$$C = \pi(B) = \{0\} \cup \pi(B \setminus B_0'). \tag{1}$$

From what we said earlier,

$$B = B_0' \cup \pi^{-1}(C \setminus \{0\}). \tag{2}$$

If $b \in B \setminus B_0'$ and $b' \in B \setminus B_0'$, one has $b + b' \in B$. From (1), C is stable for addition, and so is a subgroup of A/B_0.

Assume $B \neq B'_0$. Choose $x \in B \backslash B'_0$. One has $\pi(x) \neq 0$. Since C is a subgroup of A/B_0, there exists $y \in B \backslash B'_0$ such that $\pi(x) + \pi(y) = 0$. Then $x + y \in B_0$. For every $n \in \mathbb{N}$, one has $x + nb_0 \neq b_0$, whence $(x + nb_0) + y \in B$, i.e., $(x + y) + nb_0 \in B$. But $(x + y) + \mathbb{N}b_0 = B_0$, whence $B_0 \subset B$ and $B'_0 = B_0$. Then, using (2), $B = B_0 \cup \pi^{-1}(C \backslash \{0\}) = \pi^{-1}(C)$, and so B is a subgroup of A.

Assume $B = B'_0 \subset B_0$. One is immediately reduced to the case where $A = B_0$. So we can assume that there exists an integer $a > 0$ such that $A = \mathbb{Z}/(a)$ and $b_0 = \bar{1}$ (the bar denotes class modulo a). Assume $B \neq \{\bar{1}\}$ (if $B = \{\bar{1}\}$ the lemma is proved). Let $x_1 < x_2 < \cdots < x_k$ the integers in $[2, a]$ such that $B \backslash \{\bar{1}\} = \{\bar{x}_1, \bar{x}_2, ..., \bar{x}_k\}$. If $x_1 = a$, one has $B = \{\bar{0}, \bar{1}\}$ and the lemma is proved. Assume $x_1 < a$. One has $\bar{x}_1 + \bar{1} \in B$, and $x_1 + 1 \leqslant a$, whence $x_2 = x_1 + 1$. Step by step, we see that $B \backslash \{\bar{1}\} = \{\bar{x}_1, \overline{x_1 + 1}, \overline{x_2 + 1}, ..., \bar{a}\}$. Since $x_1 < a$, we have $a - 1 \geqslant x_1$, and so $\overline{a - 1} \in B$. Then $\overline{x - 1} = \bar{x}_1 + \overline{a - 1} \in B$. From the definition of x_1, we cannot have $\overline{x_1 - 1} \in B - \{\bar{1}\}$. So $\overline{x_1 - 1} = \bar{1}$, $x_1 = 2$, and $B = \{\bar{1}, \bar{2}, ..., \bar{a}\} = A$.

2.2. LEMMA. *Let p, q be integers > 1, $a = pq$, E and E' non-void subsets of $[1, a]$ such that*

(a) *if $x, y \in E$ are such that $x + y \leqslant a$, one has $x + y \in E$;*

(b) *$E \subset E'$, and $\mathrm{Card}(E' \backslash E) \leqslant q - 2$;*

(c) *$(E' + \mathbb{Z}p) \cap [1, a] = E'$.*

Let us denote by e the smallest element of E'. Then there are three possibilities:

(1) *$E' = \mathbb{N}e \cap [1, a]$;*

(2) *$E' = \{x, x + p, x + 2p, ..., x + (q - 1)p\}$, where $x \in [1, p - 1]$;*

(3) *$E' = \{p, 2p, 3p, ..., qp\} \cup \{x, x + p, x + 2p, ..., x + (q - 1)p\}$, where $x \in [1, p - 1]$;*

furthermore, $E \cap \{x, x + p, ..., x + (q - 1)p\} \neq \varnothing$, and every element of this set is $> a/2$.

Let $x_1 < x_2 < \cdots < x_k$ the elements of E' belonging to $[1, p]$, so that $e = x_1$. Due to hypothesis (c), one has

$$\begin{aligned} E' = \{&x_1, x_1 + p, x_1 + 2p, ..., x_1 + (q - 1)p, \\ &x_2, x_2 + p, x_2 + 2p, ..., x_2 + (q - 1)p, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &x_k, x_k + p, x_k + 2p, ..., x_k + (q - 1)p\}. \end{aligned}$$

Let i, j be integers such that $1 \leqslant i, j \leqslant k$, $i \neq j$. Consider

$$x_i, x_i + p, ..., x_i + (q-1)\, p.$$

Due to hypothesis (b), at least two of these numbers belong to E. Assume

$$x_i, x_i + p, ..., x_i + (u-1)\, p \notin E,\ x_i + up \in E$$

(one may have $u = 0$). Likewise, assume

$$x_j, x_j + p, ..., x_j + (v-1)\, p \notin E,\ x_j + vp \in E.$$

Due to hypothesis (b), one has $u + v \leqslant q - 2$. Then

$$(x_i + up) + (x_j + vp) = x_i + x_j + (u+v)\, p \leqslant 2p + (u+v)\, p \leqslant qp = a.$$

Due to hypothesis (a), one has $(x_i + up) + (x_j + vp) \in E \subset E'$. Due to hypothesis (c), $x_i + x_j \in E'$.

Furthermore, if for instance $x_i + up \leqslant x_j + vp$, one has $2(x_i + up) \leqslant a$, whence $2(x_i + up) \in E \subset E'$, whence $2x_i \in E'$.

Let $F = \{\overline{x_1}, \overline{x_2}, ..., \overline{x_k}\}$, the canonical image of E' in $\mathbb{Z}/(p)$. (The bar denotes class modulo p). We see that there exists $f_0 \in F$ such that

$$f, f' \in F \quad \text{and} \quad (f, f') \neq (f_0, f_0) \quad \Rightarrow \quad f + f' \in F.$$

From Lemma 2.1, we see that we are in one of the following cases:

(A) F is a subgroup of $\mathbb{Z}/(p)$. Then $\overline{x_2} = 2\overline{x_1}$, $\overline{x_3} = 3\overline{x_1}$, ..., $\overline{x_k} = k\overline{x_1} = 0$. So $x_2 = 2x_1$, $x_3 = 3x_1$, ..., $x_{k-1} = (k-1)\, x_1$, $x_k = kx_1 = p$. Due to hypothesis (c), $E' = \mathbb{N}x_1 \cap [1, a]$. We are in the case 1 of the lemma.

(B) $F = \{\overline{x_i}\}$ for some i. Then $k = 1$, $F = \{\overline{x_1}\}$, $E' = \{x_1, x_1 + p, x_1 + 2p, ..., x_1 + (q-1)\, p\}$. If $x_1 = p$, one has $e = p$ and we are in the case 1 of the lemma. If $x_1 < p$, we are in the case 2 of the lemma.

(C) $F = \{0, \overline{x_i}\}$ for some i such that $\overline{x_i} \neq 0$. Then $k = 2$, $x_1 < p$, $x_k = x_2 = p$, and $E' = \{x_1, x_1 + p, x_1 + 2p, ..., x_1 + (q-1)\, p, p, 2p, 3p, ..., qp\}$. Due to hypothesis (b), one has $E \cap \{x_1, x_1 + p, ..., x_1 + (q-1)\, p\} \neq \varnothing$. Let $x_1 + np$ be an element of this set such that $x_1 + np \leqslant a/2$. One has $2x_1 + 2np \in E \subset E'$ and $2x_1 \not\equiv x_1 \bmod p$, so $2x_1 \equiv 0 \bmod p$ due to the structure of E'. As $0 < 2x_1 < 2p$, we have $2x_1 = p$. So p is even, $e = x_1 = p/2$, and $E' = \mathbb{N}p/2 \cap [1, a]$. We are in the case 1 of the lemma. Finally, if every element of $E \cap \{x_1, x_1 + p, ..., x_1 + (q-1)\, p\}$ is $> a/2$, we are in the case 3 of the lemma.

2.3. LEMMA. *Let a, b be integers >0, $E \subset [1, a]$ a set of b integers, S the additive subsemigroup of $\mathbb{N}$ generated by E. Assume $b > a/2$. Then $S \supset [a-1, \infty[$.*

(This lemma is well known.)

Assume $a = 2n$ even. As $b \geqslant n+1$, one of the sets $E \cap \{1, a\}$, $E \cap \{2, a-1\}, \ldots, E \cap \{n, n+1\}$ has cardinality 2. So $i+1$, $a-i \in E$ for some i, whence $a+1 \in S$. Assume $a = 2n+1$ odd. If $n+1 \in E$, one has $a+1 = 2(n+1) \in S$. If $n+1 \notin E$, as $b \geqslant n+1$, one of the sets $E \cap \{1, a\}$, $E \cap (2, a-1)$, $E \cap \{n, n+2\}$ has cardinality 2, so again $a+1 \in S$.

So $a+1 \in S$ in all cases. Replace E by $E \cup \{a+1\}$ and a by $a+1$. This does not change S. As $b+1 > (a+1)/2$, the same argument gives $a+2 \in S$, etc. So $S \supset [a+1, \infty[$.

Assume $a-1 \notin S$ or $a \notin S$. Then Card $S \cap [1, a-2] \geqslant$ (Card $S \cap [1, a]) - 1 > (a/2) - 1$; so $S \supset [a-1, \infty[$ from the preceding result, and this is absurd. So $a-1 \in S$ and $a \in S$.

2.4. LEMMA. *Let a be an integer >0, $E \subset [1, a]$ a set of integers such that $a \in E$, and S the additive subsemigroup of $\mathbb{N}$ generated by E. For $k = 1, 2, 3, \ldots$, let $S_k = S \cap [(k-1)a+1, ka]$. Let $x \mapsto \bar{x}$ be the canonical map $\mathbb{Z} \to \mathbb{Z}/(a)$. One has*

$$\overline{S_k} + \overline{S_{k'}} \subset \overline{S_{k+k'}} \qquad \text{for all} \quad k, k'.$$

Let $x \in S_k$, $x' \in S_{k'}$. One has $x + x' \leqslant (k+k')a$, and $x+x'$, $x+x'+a$, $x+x'+2a, \ldots \in S$. One of these numbers, say $x+x'+na$, belongs to $S_{k+k'}$, and so $\bar{x} + \bar{x}' = \overline{x+x'+na} \in \overline{S_{k+k'}}$.

2.5. LEMMA. *Let S be an additive subsemigroup of $\mathbb{N}$. Let $[r, r+c]$ and $[s, s+d]$ be two intervals of integers >0, such that*

$$r \leqslant s, \qquad c \leqslant d, \qquad c+1 \in S.$$

Then Card $S \cap [r, r+c] \leqslant$ Card $S \cap [s, s+d]$.

Let τ be the translation $x \mapsto x+c+1$ from $\mathbb{N}$ to $\mathbb{N}$. We have $\tau(S) \subset S$. So Card $S \cap [r, r+c] \leqslant$ Card $S \cap [r+c+1, \ r+2c+1] \leqslant$ Card $S \cap [r+2c+2, \ r+3c+2] = \ldots$. Replacing $[r, r+c]$ by $[r+nc+n, r+(n+1)c+n]$, n well chosen, we reduce to the case where $r \leqslant s < r+c+1$. One has

$$\tau([r, s-1]) = [r+c+1, s+c]. \tag{3}$$

Note that $[r, s-1]$ may be void. Then

$$\begin{aligned}&\text{Card } S \cap [r, r+c] \\ &\quad = \text{Card } S \cap [r, s-1] + \text{Card } S \cap [s, r+c] \\ &\quad \leqslant \text{Card } S \cap [s, r+c] + \text{Card } S \cap [r+c+1, s+c] \qquad \text{due to (3)} \\ &\quad = \text{Card } S \cap [s, s+c] \leqslant \text{Card } S \cap [s, s+d].\end{aligned}$$

2.6. LEMMA. *Let a be an integer >0, A, B non-void subsets of $\mathbb{Z}/(a)$, and $C = A + B \subset \mathbb{Z}/(a)$. Let $x \mapsto \bar{x}$ be the canonical map $\mathbb{Z} \to \mathbb{Z}/(a)$. There exist integers $p, q > 0$ such that $pq = a$ and*

$$C + \mathbb{Z}\bar{p} = C$$

$$\text{Card } C \geqslant \min(a, \text{Card}(A + \mathbb{Z}\bar{p}) + \text{Card}(B + \mathbb{Z}\bar{p}) - q).$$

This is a theorem of M. Kneser (cf. [4, p. 57, Theorem 16′]).

3. PROOF OF THEOREMS 1 AND 2

3.1. LEMMA. *Let a, b, E, S, S_k be as in Theorem 2. Assume* $\max E = a$. *One has, for $k \geqslant 1$,*

$$\text{Card } S_{k+1} \geqslant \min(a, \text{Card } E + \text{Card } S_k - 1).$$

One has $E \subset S_1$, $\max S_1 = a$, $\gcd S_1 = 1$, and the subsemigroup generated by S_1 is S. As $\text{Card } S_1 \geqslant \text{Card } E$, it is enough to prove the lemma with E replaced by S_1. So we will assume $E = S_1$ from now on. In particular,

$$\text{if } x, y \in E \text{ are such that } x + y \leqslant a, \text{ one has } x + y \in E. \tag{4}$$

Let $x \mapsto \bar{x}$ be the canonical map $\mathbb{Z} \to \mathbb{Z}/(a)$. We have (Lemma 2.4)

$$\overline{S_{k+1}} \supset \bar{E} + \overline{S_k}. \tag{5}$$

According to Lemma 2.6, there exist integers $p, q > 0$ such that $a = pq$, and, setting $G = \mathbb{Z}\bar{p}$,

$$\bar{E} + \bar{S}_k + G = \bar{E} + \bar{S}_k \tag{6}$$

$$\text{Card}(\bar{E} + \overline{S_k}) \geqslant \min(a, \text{Card}(\bar{E} + G) + \text{Card}(\overline{S_k} + G) - q). \tag{7}$$

If $q = 1$, we get $\text{Card } \overline{S_{k+1}} \geqslant \min(a, \text{Card } \bar{E} + \text{Card } \bar{S}_k - 1)$, and the lemma is proved. If $p = 1$, one has $\bar{E} + \overline{S_k} = \mathbb{Z}/(a)$ from (6), whence $\overline{S_{k+1}} = \mathbb{Z}/(a)$, $\text{Card } S_{k+1} = a$, and the lemma is proved. From now on, we will assume that $p > 1$, $q > 1$, and so $p, q \leqslant a/2$.

Let $F = \bar{E}$. Assume that $\mathrm{Card}(F+G) \geqslant \mathrm{Card}\, F + q - 1$. Then

$$\mathrm{Card}(F+G) + \mathrm{Card}(\overline{S_k} + G) - q \geqslant \mathrm{Card}\, F + \mathrm{Card}\, \overline{S_k} - 1$$

and, due to (5) and (7), the lemma is proved. So from now on, we will assume that

$$\mathrm{Card}(F+G) \leqslant \mathrm{Card}\, F + q - 2. \tag{8}$$

Let E' be the set of representatives of $F+G$ in $[1, a]$. In other words, $E' = (E + \mathbb{Z}p) \cap [1, a]$. The set of representatives of F in $[1, a]$ is E. One has $\mathrm{Card}(E' \setminus E) \leqslant q-2$, due to (8). It is clear that $(E' + \mathbb{Z}p) \cap [1, a] = E'$. Due to (4), we can apply Lemma 2.2. We will consider cases (1), (2), (3) of that lemma.

Case (1). $E' = \mathbb{N}e \cap [1, a]$. Since $\gcd E = 1$, one has $e = 1$, so $E' = [1, a]$. Then $\mathrm{Card}\, E \geqslant \mathrm{Card}\, E' - (q-2) = a - q + 2 \geqslant (a/2) + 2$. Then the lemma follows from 2.3.

Case (2). This case cannot happen since $a \in E$.

Case (3). There exists $x \in [1, p-1]$ such that

$$E' = \{p, 2p, 3p, ..., qp\} \cup \{x, x+p, x+2p, ..., x+(q-1)\,p\}$$

$$E \cap \{x, x+p, ..., x+(q-1)\,p\} = \{x + s_1 p, x + s_2 p, ..., x + s_u p\}$$

with $u \geqslant 1$, $s_1 < s_2 < \cdots < s_u$, and

$$x + s_1 p > a/2. \tag{9}$$

Clearly,

$$\mathrm{Card}((E' \setminus E) \cap (x + \mathbb{Z}p)) \geqslant s_1. \tag{10}$$

Since $\gcd E = 1$, one has

$$(x, p) = 1. \tag{11}$$

Define the integer n by

$$n(x + s_1 p) \leqslant (k-1)a < (n+1)(x + s_1 p).$$

Then $(n+1)(x+s_1 p) \leqslant (k-1)a + (x + s_1 p) < ka$, and so

$$(n+1)(x+s_1 p) \in S_k \qquad (n+1)\bar{x} \in \overline{S_k}.$$

One has $n(x+s_1 p)$, $(n-1)(x+s_1 p)$, $(n-2)(x+s_1 p)$, ..., $x + s_1 p \in S \cap [1, (k-1)a]$. For $i = 0, 1, ..., n-1$, there exists an integer $t_i > 0$ such that

$(n-i)(x+s_1 p)+t_i a \in S_k$, whence $(n-i)\bar{x}+G \subset \bar{S}_k+G$. If $n+1 \geqslant p-1$, we deduce that

$$G, \bar{x}+G, 2\bar{x}+G, ..., (p-1)\bar{x}+G \subset \bar{S}_k+G,$$

whence $\bar{S}_k+G=\mathbb{Z}/(a)$ due to (11). Then, using (5) and (6),

$$\overline{S_{k+1}} \supset \bar{E}+\overline{S_k}=\bar{E}+\overline{S_k}+G=\bar{E}+\mathbb{Z}/(a)=\mathbb{Z}/(a),$$

and the lemma is proved. So, from now on, we will assume that

$$n \leqslant p-3. \tag{12}$$

Due to (11), every element of S which is congruent to $(n+1)x$ modulo p is of the form $n'(x+s_1 p)+tp$, where t is a nonnegative integer and $n' \equiv n+1 \bmod p$. Due to (12), one has $n' \geqslant n+1$, and so $n'(x+s_1 p)+tp \geqslant (n+1)(x+s_1 p)$. So $(n+1)(x+s_1 p)$ is the smallest element of $S \cap ((n+1)x+\mathbb{Z}p)$. So

$$S_k \cap ((n+1)x+\mathbb{Z}p) \cap [(k-1)a+1, (n+1)(x+s_1 p)-1] = \varnothing \tag{13}$$

and one proves in the same way that

$$S_k \cap ((n+2)x+\mathbb{Z}p) \cap [(k-1)a+1, (n+2)(x+s_1 p)-1] = \varnothing. \tag{14}$$

First case. One has

$$n(x+s_1 p) \leqslant (k-1)a < (n+1)(x+s_1 p) < ka < (n+2)(x+s_1 p). \tag{15}$$

Then

$$\begin{aligned}
&(n+1)(x+s_1 p)-((k-1)a+1) \\
&\quad = a-(ka-(n+1)(x+s_1 p))-1 \\
&\quad \geqslant a-((n+2)(x+s_1 p)-(n+1)(x+s_1 p)-1)-1 \qquad \text{due to (15)} \\
&\quad = a-(x+s_1 p) = p(q-s_1)-x \geqslant p(q-s_1-1).
\end{aligned} \tag{16}$$

If h is a positive integer, one has

$$\begin{aligned}
h \leqslant q-s_1-1 \quad &\Rightarrow \quad hp \leqslant (n+1)(x+s_1 p)-((k-1)a+1) \\
&\qquad \text{due to (16)} \\
&\Rightarrow \quad (k-1)a+1 \leqslant (n+1)(x+s_1 p)-hp \leqslant ka \\
&\qquad \text{due to (15)} \\
&\Rightarrow \quad (n+1)(x+s_1 p)-hp \in ((S_k+\mathbb{Z}p) \\
&\qquad \cap [(k-1)a+1, ka]) \backslash S_k
\end{aligned}$$

due to (15) and (13). We deduce that

$$h \leqslant q - s_1 - 1 \qquad \Rightarrow \qquad (n+1)(\bar{x} + s_1 \bar{p}) - h\bar{p} \in (\bar{S}_k + G) \backslash \bar{S}_k$$

and so

$$\operatorname{Card}((\bar{S}_k + G) \backslash \bar{S}_k) \geqslant q - s_1 - 1. \tag{17}$$

Then, using (5), (7), (10), (17), we get

$$\begin{aligned} \operatorname{Card} \overline{S_{k+1}} &\geqslant \min(a, \operatorname{Card} \bar{E} + s_1 + \operatorname{Card} \overline{S_k} + q - s_1 - 1 - q) \\ &= \min(a, \operatorname{Card} \bar{E} + \operatorname{Card} \overline{S_k} - 1). \end{aligned}$$

Second case. One has

$$n(x + s_1 p) \leqslant (k-1)a < (n+1)(x + s_1 p) < (n+2)(x + s_1 p) \leqslant ka.$$

Then

$$\begin{aligned} &(n+2)(x + s_1 p) - ((k-1)\, a + 1) \\ &\quad \geqslant (n+2)(x + s_1 p) - (n+1)(x + s_1 p) \\ &\quad = x + s_1 p \geqslant a - (x + s_1 p) \qquad \text{due to (9)} \\ &\quad = p(q - s_1) - x \geqslant p(q - s_1 - 1). \end{aligned}$$

We end the proof as in the first case, replacing everywhere $n+1$ by $n+2$.

3.2. LEMMA. *Let a, b, E, S, S_k be as in Theorem 2. Assume* $\max E = a$. *One has, for* $k \geqslant 1$,

$$\operatorname{Card} S_k \geqslant \min(a, kb - k + 1).$$

This is clear for $k = 1$. We get the general case by induction on k, using 3.1.

3.3. *Proof of Theorem* 2. Let a, b, E, S, S_k be as in Theorem 2. Let $a' = \max E$, and $T_k = S \cap [(k-1)\, a' + 1, ka']$. From 3.2, we have

$$\operatorname{Card} T_k \geqslant \min(a', kb - k + 1). \tag{18}$$

If $\operatorname{Card} T_k = a'$, we have $S \supset [(k-1)\, a' + 1, \infty[$ (Lemma 3.1), so $\operatorname{Card} S_k = a$ and the theorem is proved. Assume $\operatorname{Card} T_k < a'$. From (18), we have $\operatorname{Card} T_k \geqslant kb - k + 1$. Due to 2.5, $\operatorname{Card} S_k \geqslant \operatorname{Card} T_k$. So $\operatorname{Card} S_k \geqslant kb - k + 1$ and the theorem is proved.

3.4. *Proof of Theorem* 1. Let a, b be integers such that $2 \leqslant b \leqslant a$.

(A) Let $k = \lceil (a-1)/(b-1) \rceil$. One has $k(b-1) \geqslant a-1$, whence $kb - k + 1 \geqslant a$. Let $E \subset [1, a]$ be a set of b integers, such that $\gcd E = 1$. Let S be the subsemigroup generated by E. For $j \geqslant k$, Theorem 2 gives Card $S \cap [(j-1)a+1, ja] = a$. So $S \supset [(k-1)a+1, \infty[$. If $a \in S$, one has even $S \supset [(k-1)a, \infty[$. If $a \notin S$, let $a' = \sup S \cap [1, a]$. The preceding argument gives $S \supset [(k-1)a', \infty[\supset [(k-1)a, \infty[$. So $G(E) \leqslant (k-1)a - 1 = (\lceil (a-1)/(b-1) \rceil - 1)a - 1$, and $g(b, a) \leqslant (\lceil (a-1)/(b-1) \rceil - 1)a - 1$.

(B) Let us take $E = \{a-b+1, a-b+2, ..., a\}$. One has, for $j = 1, 2, ...,$

$$S_j = [ja - jb + j, ja] \cap [(j-1)a + 1, ja].$$

Let $k' = \lfloor (a-2)/(b-1) \rfloor$. Assume $a > b$. Then $k' \geqslant 1$. One has $k'(b-1) \leqslant a-2$, whence

$$k'a - k'b + k' \geqslant k'a - a + 2 > (k'-1)a + 1.$$

So $G(E) \geqslant k'a - k'b + k' - 1$ (this is remarked in [1]) and we deduce that $g(b, a) \geqslant k'a - k'b + k' - 1$.

3.5. THEOREM 3. *Let a, b be integers with $2 \leqslant b < a$. Let the integers k and r be defined by*

$$a - 1 = k(b-1) - r \qquad 0 \leqslant r < b - 1$$

so that $k = \lceil (a-1)/(b-1) \rceil$. Then $g(b, a) \leqslant (k-1)(a-r-1) - 1$.

(This improves the 2nd inequality in Theorem 1.)

Let E and S be as in the proof of Theorem 1. For $j \leqslant k-1$, one has

$$jb - j + 1 \leqslant (k-1)(b-1) + 1 = a - 1 + r - b + 1 + 1 = a - (b - 1 - r) < a.$$

So, by Theorem 2,

$$\text{Card } S \cap [(j-1)a + 1, ja] \geqslant jb - j + 1.$$

We deduce that

$$\begin{aligned} \text{Card } S \cap [1, (k-1)a] &\geqslant \tfrac{1}{2}k(k-1)(b-1) + (k-1) \\ &= \tfrac{1}{2}(k-1)(a-1+r) + (k-1) = \tfrac{1}{2}(k-1)(a+r+1), \end{aligned}$$

whence

$$\begin{aligned}&\text{Card } S \cap [1, (k-1)(a-r-1)+1] \\ &\quad = \text{Card } S \cap [1, (k-1)a-(k-1)(r+1)+1] \\ &\quad \geqslant \tfrac{1}{2}(k-1)(a+r+1)-(k-1)(r+1)+1 \\ &\quad = \tfrac{1}{2}((k-1)(a-r-1)+1)+\tfrac{1}{2}.\end{aligned}$$

From Lemma 2.3, we deduce $S \supset [(k-1)(a-r-1), \infty[$, so that $G(E) \leqslant (k-1)(a-r-1)-1$, and $g(b, a) \leqslant (k-1)(a-r-1)-1$.

3.6. THEOREM 4. *If $b-1$ divides a or $a-2$, one has*

$$g(b, a) = \frac{a(a-2)}{b-1} - a + 1.$$

Assume that $b-1$ divides $a-2$. Set $t=(a-2)/(b-1)$. Then $a-1=(t+1)(b-1)-(b-2)$, and so, with the notations of Theorem 3, $k=t+1$ and $r=b-2$. So, by Theorem 3, $g(b, a) \leqslant t(a-(b-2)-1)-1 = ta-t(b-1)-1 = ta-(a-2)-1 = ta-a+1$. But, by Theorem 1, $g(b, a) \geqslant ta-(a-2)-1 = ta-a+1$. So $g(b, a) = ta-a+1 = (a-2)/(b-1)\, a-a+1$.

Assume that $b-1$ divides a. Set $s=a/(b-1)$. Then $a-1=s(b-1)-1$. We can apply Theorem 3 (except if $b=2$, but the theorem is evident for many reasons in that case); with the notations of that theorem, $k=s$ and $r=1$. So $g(b, a) \leqslant (s-1)(a-2)-1$. Let $E=\{s, 2s, 3s, ..., (b-2)s, a-1, (b-1)s=a\}$. We have $\sup E=a$, $\gcd E=1$, $\text{Card } E=b$. Then the greatest integer not in S is, according to [5, Sect. 5], $(s-1)(a-2)-1$. So

$$g(b, a) = (s-1)(a-2)-1 = (a/(b-1))(a-2)-a+1.$$

3.7. THEOREM 5. *If $b-1$ divides $a-1$, one has*

$$g(b, a) = ((a-1)^2/b-1)-a.$$

With the notations of Theorem 3, $k=(a-1)/(b-1)$ and $r=0$, so

$$g(b, a) \leqslant (k-1)(a-1)-1 = ka-k-a.$$

Let $E=\{k, 2k, 3k, ..., (b-1)k, a\}$; note that $a=(b-1)\,k+1$. We have $\max E=a$, $\gcd E=1$, $\text{Card } E=b$. Then, as in [5, Sect. 5], we see that $G(E)=ka-a-k$. So $g(b, a)=ka-k-a=k(a-1)-a=((a-1)^2/(b-1))-a$.

3.8. Theorems 4 and 5 prove Lewin's conjecture [5, Sect. 5] when $b-1$ divides a or $a-1$ or $a-2$; they give the exact value of $g(2, a)$ (trivial anyway), of $g(3, a)$ (already obtained in [5]), and of $g(4, a)$ (already obtained in [6]). The first case where the exact value is not obtained is the case $b=5$, $a \equiv 3 \bmod 4$.

3.9. In all cases of Theorems 4 and 5, the exact value of $g(b, a)$ is equal to the upper bound of Theorem 3. But this is not true in general. For instance, $g(5, 11)=13$ (resp. $g(5, 15)=32$) (case by case checking) and the upper bound of Theorem 3 is 15 (resp. 35).

ACKNOWLEDGMENT

I thank the referee for several useful remarks.

REFERENCES

1. A. BRAUER, On a problem of partitions, *Amer. J. Math.* **64** (1942), 299–312.
2. P. ERDŐS AND R. L. GRAHAM, On a linear diophantine problem of Frobenius, *Acta Arith.* **21** (1972), 399–408.
3. P. ERDŐS AND R. L. GRAHAM, "Old and New Problems and Results in Combinatorial Number Theory," Monographies de l'Enseignement Mathématique, No. 28, Université de Genève, 1980.
4. H. HALBERSTAM AND K. F. ROTH, "Sequences," Oxford Univ. Press, London/New York, 1966.
5. M. LEWIN, A bound for a solution of a linear diophantine problem, *J. London Math. Soc.* **6** (1972–1973), 61–69.
6. Y. VITEK, Bounds for a linear diophantine problem of Frobenius, II, *Canad. J. Math.* **28** (1976), 1280–1288.